

Meeting	Audit Committee	Date	08/09/2014
Agenda item	7	Time	10 Minutes
Proactive publication	Yes	Internal publication	Yes
Title	<b>Reporting of fraud, whistleblowing and security incidents</b>		
Presenter	Peter Bloomfield		
ICO Plan aim	6. An efficient ICO well prepared for the future		
Information rights strategy aim	10. The public confident in information rights law as necessary, serving the public interest, effective in practice and properly enforced.		
Issue	At the last Audit Committee I took an action to advise on the reporting of fraud, whistleblowing and security incidents. Attached are the relevant procedures with this paper highlighting current formal reporting mechanisms.		
Decision	<p>Do these procedures provide the right level of assurance to the Committee and management?</p> <p>General comments are also welcome on the various procedures detailed in the paper.</p>		
Financial impact	Not relevant.		
Risks	Not relevant.		

## Current reporting procedures

The ICO has the following policies and procedures:

- Staff code of conduct (annex A)
- Fraud response plan (annex B)
- Whistleblowing policy and procedure (annex C)
- Security Manual (the *Security Incidents* section is at Annex D).

Within these documents there are reporting mechanisms:

- **Staff code of conduct**
  - Concerns about improper conduct are to be reported to line managers or one of the deputy commissioners.
  - If however the individual is concerned that the above are supportive of the conduct then the following are listed as possible contacts:
    - Chair of the Audit Committee
    - Internal or external auditors
    - The MoJ.
- **Fraud response plan**
  - On discovery of the fraud the fraud should be reported to one of the deputy commissioners (para 5.1).
  - Subsequently the Commissioner should be informed and he is responsible for advising the MOJ, the internal auditors and the Audit Committee.
- **Whistleblowing policy and procedure**
  - Concerns should be reported to line managers, their manager, the Head of Finance, the Information Governance Team or ultimately a member of Executive Team.
  - If however the individual is concerned that the above are supportive of the conduct then the following are listed as possible contacts:
    - Chair of the Audit Committee
    - Internal or external auditors
    - The MoJ
- **Security Manual**
  - To line managers and then on to other parties as appropriate (last page of annex D)
  - The Information Governance Group Manager reports quarterly to the Information Governance group on security incidents.

Before each Audit Committee the Head of Organisational Development and the Head of Finance are asked if there have been any incidents of fraud reported to them since the last meeting. There have been none reported prior to this meeting.

Peter Bloomfield  
Corporate Governance

# Code of conduct

The Committee on Standards in Public Life chaired by Lord Nolan, recommended in its First Report that each executive Non-Departmental Public Body should adopt a Code of Conduct for its staff. The recommendation arose from the view that there was a need for clear expectations of standards to be set out, and a concern that public office should not be misused to pursue personal interest.

The Committee recommended that each Non-Departmental Public Body should nominate an official or board member who would be entrusted with the duty of investigating staff concerns about issues raised confidentially. The Deputy Commissioner has been nominated as the person who will investigate concerns on matters of propriety raised confidentially, with the possibility of final appeal to the Commissioner. The statutory position of the Commissioner means that there could not be an appeal to anyone outside the organisation. However, in exceptional circumstances where it is felt that staff concern might be for example that those with whom they might raise the issue were a party to, or supportive of, the behaviour causing concern, it has been agreed with the Ministry of Justice (MOJ) that they will provide an avenue of address outside the Office.

The Code has no legal force, although it forms part of your terms and conditions of service, breaches of which may be the subject of disciplinary action.

## **Duties and responsibilities**

You are asked to familiarise yourself with the contents of the Code and act in accordance with the principles set out in it.

### **You have a duty to:**

- a) discharge public functions reasonably and according to the law; and
- b) recognise ethical standards governing particular professions.

### **You should be aware:**

- a) of your accountability to the Commissioner whom you serve; and
- b) of the respective roles of the sponsor department and the Commissioner as set out in the Management Statement, and Memorandum on Payment of Grant-in-Aid; and
- c) that the Commissioner is ultimately accountable to Parliament for his or her independence, effectiveness and efficiency.

You are asked to conduct yourself at all times with integrity, impartiality

and honesty. You should not deceive or knowingly mislead the Commissioner, the Ministry of Justice, Ministers, Parliament or the Public.

### **Conflicts of interest**

You should abide by the rules adopted by the Commissioner in relation to private interest and possible conflict with public duty; the disclosure of official information; and political activities.

You should not misuse your official position or information acquired during the course of your duties to further your private interests or those of others. If you are a member of the senior management group, or a member of staff who is either working on a contract or dealing with issues which could raise matters of substance, you should ensure that any possible conflicts of interest are identified at an early stage and that appropriate action is taken to resolve them.

If you have any doubts about possible conflicts of interests, you should, in the first instance discuss your concerns with either the Human Resources Manager or the Human Resources Director .

### **Integrity**

You should not use your official position to receive, agree to accept or attempt to obtain any payment or other consideration for doing, or not doing, anything or showing favour, or disfavour, to any person. You should not receive benefits of any kind from a third party which might reasonably be seen to compromise their personal judgement and integrity. Under the Prevention of Corruption Act 1916, you may as an employee of the Commissioner be required to prove that the receipt of payment or other consideration from someone seeking to obtain a contract is not corrupt.

### **Relations with the public**

If during the course of your duties you are required to deal with the affairs of the public you should do so sympathetically, efficiently, promptly and without bias or maladministration. At all times you should offer the public the highest standards of conduct and service.

### **Effective use of resources**

You should endeavour to ensure the proper, economical, effective and efficient use of resources.

### **Official information**

Under common law you are required to undertake a general duty of confidentiality. You are required to protect official information held in confidence. Nothing in the Code should be taken as overriding existing statutory or common law obligations to keep confidential, or in appropriate cases to disclosure, certain information. Subject to this

provision, staff should act in accordance with the "Code of Practice on Access to Government Information: Procedures for implementation within the Information Commissioner's Office."

### **Staff concerns about improper conduct**

If you believe you are being required to act in a way which:

- is illegal, improper, or unethical;
- is in breach of a professional code;
- may involve possible maladministration, fraud or misuse of public funds;
- is otherwise inconsistent with this Code;

You should either raise the matter through the management line or else approach in confidence one of the Deputy Commissioners who are entrusted with the duty of investigating staff concerns about illegal, improper or unethical behaviour. You should also draw attention to cases where there is evidence of irregular or improper behaviour elsewhere in the organisation, but where you have not been personally involved, or if you are required to act in a way which, for you, raises a fundamental issue of conscience.

If you have reported a matter covered in the above paragraph and believe that the response does not represent a reasonable response to the grounds of your concern, you may report the matter directly to the Commissioner. If you feel that the people within the office with whom you could normally raise the issue are parties to, or supportive of, the behaviour causing concern, you may report the matter to the chair of the ICO's Audit Committee or to representatives of our auditors.

- The chair of the ICO's Audit Committee is Ian Watmore. Ian Watmore is a non-executive member of the ICO's management board.
- Our internal auditors, Grant Thornton, contact details for whom can be obtained from Corporate Governance.
- Our external auditors, the National Audit Office, contact details for whom can be obtained from Corporate Governance.
- Our sponsor department, the Ministry of Justice, contact details for whom can be obtained from Corporate Governance.

Who have been nominated by our Sponsor Department to investigate such issues.

### **After leaving the Commissioner's employment**

You should continue to observe your duty of confidentiality after you have left the employment of the Commissioner.

### **Political activities**

The ICO has a policy and procedure regarding party political activities. If you are involved in such activity it is essential to read and comply with this policy to help ensure that the ICO's impartiality and independence is retained. The policy can be found on the staff intranet under policies and procedures or click the link **Political Activities Policy**.

**Staff information**

# Fraud response plan

## **1. Introduction**

- 1.1. This plan deals mainly with the responsibilities of all staff in deterring losses to public funds. There are additional responsibilities borne by managers. The document deals mainly with the internal response and actions that we need to take within the Office to both deter fraud, and to respond to any suspicion of it that comes to our attention. That said, it is important to remember that fraud could be carried out by people outside the Office and we each of us need to be aware of this in our dealings with external parties.
- 1.2. Any suspicion of 'fraud' will be investigated as set out in this plan. Any proven instance of fraud will result in disciplinary action being taken against any member of staff involved. The policy of the Commissioner is to notify the police in circumstances where there is evidence that a crime may have been committed.
- 1.3. The staff code of conduct sets out standards which staff are expected to meet at all times, particularly with regard to the safeguarding of public funds.

## **2. What is fraud?**

- 2.1. For practical purposes, so far as this document is concerned, fraud may be taken to mean the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to another party.
- 2.2. The essential elements of fraud are dishonesty, which can include non-disclosure of important facts, and deprivation or risk of deprivation.
- 2.3. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

## **3. Responsibilities**

- 3.1. Individual members of staff are responsible for -
  - Acting with propriety in the use of official resources and in the handling and use of public funds, whether they are involved with cash or payments systems, receipts or dealing with contractors or suppliers.

- Reporting immediately to their line manager or next most senior manager if they suspect that a fraud has been committed or see any suspicious acts or events.

3.2. In addition to those individual responsibilities, managers are responsible for –

- Identifying the risks to which systems and procedures are exposed.
- Developing and maintaining effective controls to prevent and detect fraud
- Ensuring that controls are complied with

#### **4. Objectives of this Plan**

4.1. The objectives of having a widely circulated and understood response plan are

- To deter fraud by publicising steps that will be taken if any is discovered
- To set out managers' responsibilities in this area
- To set out clear guidance on the appropriate steps to be taken if managers become aware of, or suspect that, fraud may be taking place

4.2. The steps set out in the Plan have been devised with the aims of

- Minimising delay in taking any appropriate action
- Reducing the impact of any fraud which takes place
- Ensuring that any possible frauds are investigated
- Preventing or minimising losses of funds
- Maximising the possibility and amounts of recovery
- Identifying perpetrators of fraud and increasing the likelihood of successful disciplinary or legal action
- Minimising the possibility of adverse publicity
- Ensuring that lessons learned from any instances of suspected fraud are acted upon.

#### **5. Reporting**

5.1. Immediately that fraud is discovered or suspected, the matter should be reported to one of the Deputy Commissioners (David Smith or Graham Smith), substitute nominated by them, who will decide what further action is appropriate.

## **6. Immediate Considerations and Actions**

6.1. The primary objective should be to ensure that public funds are protected. So, the initial investigation should attempt to determine whether there is any possibility of further offences taking place. If there is thought to be any possibility of recurrence, then actions which should be considered include

- freezing bank accounts
- suspending BACS or cheque payments
- suspending individuals

## **7. Enquiries**

7.1. Enquiries into the possibility of fraud taking place should be begun without delay. Facts need to be established, steps taken to protect any individual who may have been unwittingly involved and to ensure that any evidence that is discovered can be used in any subsequent action that might be necessary. To assist in this, it may be appropriate to involve the Police where there is evidence that a criminal offence may have taken place.

## **8. Recovery Action**

8.1. Prompt action is likely to be important in maximising recovery of any funds which have been lost or are thought to be vulnerable as a result of the fraud

8.2. Consideration should be given to involving other parties such as

- the Bank Manager to discuss the desirability or possibility of recalling BACS/CHAPS payments, cancelling cheque payments or withdrawing and replacing pre-printed payment stationery.
  - a legal adviser for advice on recovery of other assets

## **9. Reporting Action**

9.1. The circumstances of the fraud and action taken should be reported to the Information Commissioner (Christopher Graham). He will be responsible for

- Reporting the matter to our Sponsor Unit at the Ministry of Justice
- Reporting the incident in any required returns
- Reporting the matter to our internal auditors and the Audit Committee

## **10. Disciplinary/Legal Action**

10.1. Where evidence of fraud is discovered and those responsible can be identified -

- Appropriate disciplinary action will be taken in line with the disciplinary procedure, which is set out in the Staff Handbook.
- When legal action is considered appropriate, full co-operation will be given to investigating and prosecuting authorities.

## **11. Further Action**

11.1. A full report on the circumstances and outcome of any fraud or suspected fraud will be produced. The report will cover the identification of any shortfall in current procedures which contributed to the commission, recommendations on actions which could be taken to prevent or reduce the effect of any future occurrence and who will be responsible for considering these.



# ‘Speak up’ – The ICO’s whistleblowing policy and procedure

<b>1. Scope</b>	
1.1	All employees of the Information Commissioner's Office (ICO) and other workers undertaking activity on behalf of the ICO.
<b>2. Purpose</b>	
2.1	To prevent malpractice by the organisation, its employees, agents and partners by advising staff how to raise concerns with the organisation's management or, if necessary, with its sponsoring department and advising them of the protection offered by the Public Interest Disclosure Act 1998 ('PIDA').
<b>3. Introduction</b>	
3.1	All organisations face the risk of things going wrong or of unknowingly harbouring malpractice. We have a duty to identify and take measures to remedy all malpractice particularly with regard to issues of fraud and corruption.
3.2	By encouraging a culture of openness within our organisation we believe that we can prevent malpractice before it happens.
3.3	By promoting a culture of openness we want to encourage you to raise issues which concern you at work. We recognise, however, that you may be worried that by reporting such issues you will be opening yourself up to victimisation, detriment or risking your job security.
3.4	Such fears are understandable, this policy is therefore designed provide you with information about the protections offered by PIDA as well as the process by which you may raise your concerns.
3.5	By knowing about malpractice at an early stage we stand a good chance of taking the necessary steps to safeguard the interests of all staff, protect our organisation and stop fraud and corruption before it happens.
3.6	In short, do not hesitate to 'speak up' or 'blow the whistle' on malpractice.
<b>4. Definitions</b>	
4.1	<p>'Fraud': for the purpose of this policy refers to where an individual has undertaken, or intends to undertake, actions in order to obtain gain for him/herself or another, or cause loss to another, or expose another to risk of loss.</p> <p>The term 'fraud' encompasses:</p> <ul style="list-style-type: none"> <li>i) Fraud by false representation;</li> <li>ii) Fraud by failing to disclose information; and</li> </ul>

iii) Fraud by abuse of position.

Descriptions of the above can be found within the Fraud Act 2006.

4.2 'Corruption' for the purpose of this policy refers to an individual who has given or obtained advantage through means which are illegitimate, immoral, and/or inconsistent with their duty to the ICO or the rights of others. Examples include accepting bribes or incentives during procurement processes, seeking to influence others

4.3 'Malpractice' for the purpose of this policy refers to actions which may be:

- i) illegal, improper, or unethical;
- ii) in breach of a professional code;
- iii) possible maladministration, fraud or misuse of public funds; or
- iv) acts which are otherwise inconsistent with the Staff Code of Conduct.

## 5. Grievances

5.1 It should be noted that this policy is not our normal grievance procedure. If you have a complaint about your own personal circumstances then you should use the grievance procedure. If you have concerns about malpractice within the organisation then you should use the procedure outlined in this policy.

## 6. Protection of whistleblowers

6.1 The management of the ICO is committed to this policy. If the policy is used to raise a concern in good faith we give you our assurance that you will not suffer any form of retribution, victimisation or detriment as a result of your actions. In addition, the PIDA may provide you with legal protection in relation to your disclosures if you raise your concerns in accordance with that Act.

6.2 Concerns will be treated seriously and actions taken in accordance with this policy. If you ask us to treat the matter in confidence we will do our utmost to respect your request. However, it is not possible to guarantee confidentiality. If we are in a position where we cannot maintain confidentiality and so have to make disclosures we will discuss the matter with you first. We will give you feedback on any investigation and be sensitive to any concerns you may have as a result of any steps taken under this procedure.

6.3 In some circumstances the ICO may decide that we ought to reveal your identity in order to assist in the investigation into the matter. You will be advised beforehand if this is the case.

6.4 Remember, if you do not tell us who you are it will be much more difficult for us to look into the matter, to protect your position or to

give you feedback. Accordingly, while we will consider anonymous reports, this procedure is not appropriate for concerns raised anonymously.

- 6.5 Whistleblowers receive protection under the PIDA. Further information about the protection afforded under PIDA can be found using the resources listed at the end of this policy.

## 7. Procedure

### 7.1 **Tell your line manager**

If you are concerned about any form of malpractice you should normally first raise the issue with your line manager. There is no special procedure for doing this - simply tell them about the problem or put it in writing if you prefer.

At whatever level you raise the issue, you should declare whether you have a personal interest in the issue at the outset. If your concern falls more properly within the grievance procedure your manager will tell you.

### 7.2 **If you feel unable to tell your line manager**

If you feel you cannot tell your line manager, for whatever reason, you should raise the issue with the next tier of management or, if the issue is related to financial issues, the Head of Finance. If you feel that the issue concerns issues of compliance with the legislation regulated by the ICO, you may speak with the Head of Internal Compliance.

If you feel that you cannot disclose to the next tier of management, Head of Finance or Head of Internal Compliance because you believe that the individual may be implicated in the malpractice you should raise the matter in confidence with one of the Executive Team.

The Executive Team are entrusted with the duty of investigating staff concerns about illegal, improper or unethical behaviour.

You should also approach one of the Executive Team to draw attention to cases where there is evidence of irregular or improper behaviour elsewhere in the organisation, but where you have not been personally involved, or if you are required to act in a way which, for you, raises a fundamental issue of conscience.

### 7.3 **If you still have concerns**

If you have reported a matter as described in the above paragraph and believe that the response does not represent a reasonable response to the issues you have raised, you may report the matter directly to the Commissioner.

### 7.4 **If you feel unable to raise the matter within the ICO**

If you feel that the people within the office with whom you could normally raise the issue are parties to, or supportive of, the behaviour causing concern, you may report the matter to the chair of the ICO's Audit Committee or to representatives of our auditors.

- The chair of the ICO's Audit Committee is Ian Watmore. Ian Watmore is a non-executive member of the ICO's management board.
- Our internal auditors, Grant Thornton, contact details for whom can be obtained from Corporate Governance or found on the Internal Audit Plan which is published on ICON.
- Our external auditors, the National Audit Office, contact details for whom can be obtained from Corporate Governance.
- Our sponsor department, the Ministry of Justice, contact details for the ICO's liaison team can be obtained from Corporate Governance.

## 7.5 **Responding to whistleblowing**

After you have raised your concern we will decide how to respond in a responsible and appropriate manner. Usually this will involve making internal enquiries first but it may be necessary to carry out an investigation at a later stage which may be formal or informal depending on the nature of the concern raised.

If you have raised a concern we will, as far as possible, keep you informed of the decisions taken and the outcome of any enquiries and investigations carried out. However, we will not be able to inform you of any matters which would infringe our duty of confidentiality to others.

## 7.6 **Raising your concern externally (exceptional cases)**

In all but the most exceptional of circumstances concerns about malpractice should be raised internally or with the representatives of our sponsoring department.

The purpose of this policy is to give you the opportunity and protection you need to raise your concerns internally without reporting the concern to external bodies. It is, therefore, expected that raising concerns internally will be the most appropriate action to be taken in almost all cases and so you must try to do so.

If, however, you feel you cannot raise your concerns internally the PIDA may afford you protection in relation to your disclosure but only if you are acting in good faith and if you honestly and reasonably believe that your allegations are true. In such circumstances you may consider raising the matter with the police or the appropriate

regulator e.g. Health and Safety Executive, Environmental Health Department etc. If you do take this route to whistleblow an issue you may be required to demonstrate why you thought the normal internal procedure was not appropriate.

You are strongly recommended to take advice (see section 7.9 below) before following this course of action though, as the PIDA only affords protection to whistle blowers in certain circumstances.

### 7.7 **Wider whistleblowing disclosures**

If you have good reason for not using the internal or regulatory disclosure procedures described above, you might consider making wider disclosure by reporting the matter to the media, or making a posting on the internet.

Please note, if you have not followed internal procedures, whistleblowing disclosures to the media or by other public disclosure will generally be considered to be an unreasonable course of action. Reporting your concerns for public circulation, even if done in good faith, before raising them in accordance with these procedures may result in disciplinary proceedings, which could lead to dismissal.

You are recommended to take legal advice before following this course of action though, as the PIDA only affords protection to whistle blowers in certain circumstances. In particular, no protection is given if the disclosure is made for personal gain.

### 7.8 **Limits to protection**

It is important to note that a disclosure will not be protected under PIDA where you are committing an offence by making that disclosure, for example by breaching the Official Secrets Act or Section 59 of the Data Protection Act.

### 7.9 **Sources of advice**

It is recommended to that you obtain advice about whistleblowing and PIDA at an early stage if you intend to report malpractice. This is important so that you know the extent of the protection which will be provided to you under PIDA.

If you are a member of a trade union you may wish to seek advice about raising an issue from a trade union representative. You may also wish to seek advice from Public Concern at Work which is an independent charity set up to provide advice and guidance about whistleblowing issues. Contact details for Public Concern at Work are given in Section 9.

## **8. Malicious whistleblowing**

**8.1** If you are found to have made allegations maliciously and/or not in good faith, a disciplinary process may be instigated against you. This may result in your dismissal from the ICO.

**8.2** It is important to note that as long as you have raised a concern in good faith, you will not be subject to disciplinary action even if the investigation finds your allegations to be unproven.

## 9. Frequently asked questions

**9.1 I told my line manager a number of weeks ago that I believe that a colleague is misusing ICO resources. Nothing seems to have happened since. What should I do?**

Speak with your line manager to ask how the investigation is progressing. If you feel that no or insufficient progress has been made you must inform your manager's manager.

**9.2 I have serious concerns that malpractice is prevalent within my team and that my manager and the more senior managers know about the situation but have chosen to ignore it. What should I do?**

You must contact the Commissioner personally and inform him/her of your concerns. If you feel the Commissioner is involved in, or supportive of, the malpractice you should raise the matter with the representatives of our sponsor department as detailed in the procedure above.

**9.3 I believe that a colleague is stealing from the ICO. How do I deal with this?**

This issue should be dealt with by using this whistleblowing procedure. You must, therefore, inform your line manager.

**9.4 I believe that malpractice is happening within the ICO and I am thinking of going to the press about it. What are the implications of this?**

You should try to exhaust all internal mechanisms for whistleblowing or refer to our sponsoring department or the relevant regulatory body. You should be aware that going directly to the press may limit your protection under the Public Interest Disclosure Act (PIDA) and you may be liable for dismissal. It is advised that you seek advice from your trade union, if you are a member, or contact Public Concern at Work (whose details are in section 9) before taking this course of action.

**9.5 What does PIDA do?**

PIDA protects workers who make a **protected disclosure** of information, concerning certain types of matters relating to their employment, from being dismissed or penalised by their employers as

a result of the disclosure.

## 9.6 Who may claim the protection of PIDA?

Members of staff are **workers** within the definition contained in PIDA and may make a qualifying disclosure of information if they reasonably believe that the disclosure would tend to show that the ICO is involved in a **relevant failure** as outlined in section 9.7 below.

## 9.7 What disclosures are protected?

Not all disclosures of information are protected by PIDA. Protection only arises in relation to **protected disclosures**. **Protected disclosures** are:

- **qualifying disclosures** (defined below) made to an appropriate party (see section 9.8. below); and
- made in accordance with the differing conditions for disclosure applying to each different type of recipient of the information.

A **qualifying disclosure** is:

"any disclosure of information which, *in the reasonable belief of the worker making the disclosure*, tends to show one or more of the following.

(a) That a criminal offence has been committed, is being committed or is likely to be committed;

(b) That a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject;

(c) That a miscarriage of justice has occurred, is occurring or is likely to occur;

(d) That the health or safety of any individual has been, is being or is likely to be endangered;

(e) That the environment has been, is being or is likely to be damaged; or

(f) That information tending to show any matter falling within any one of the preceding paragraphs has been, or is likely to be deliberately concealed."

PIDA refers to those matters covered by (a) to (f) above as **relevant failures**.

A disclosure will not be a qualifying disclosure if the person making it commits an offence by making it (e.g. if the disclosure would breach

official secrets legislation or if it would breach section 59 DPA 1998). You would therefore not receive protection under PIDA if you made a disclosure in these circumstances.

### 9.8 To whom may a disclosure be made?

A protected disclosure may be made to one of five types of recipients, these are:

- the worker's employer;
- a legal adviser;
- a Minister of the Crown (in certain circumstances);
- a regulatory body (referred to as a prescribed person – including the Information Commissioner); and
- a third party (for example, the media).

The circumstances in which disclosures may be made vary depending upon the intended recipient of the information.

The most likely recipient of information from ICO staff concerning misconduct will be the ICO **as the employer** of the worker in question. To be protected by PIDA, a worker wishing to make a disclosure must make sure that s/he reasonably believes that the disclosure tends to show a **relevant failure** and s/he must make the disclosure in good faith.

You may need independent legal advice to direct you in understanding this legislation.

## 10. Resources

- 10.1 For more information on whistleblowing and related legislation visit: <http://www.pcaw.co.uk>

If you need independent advice about a whistleblowing issue you can telephone Public Concern at Work on 020 7404 6609.

Further information about PIDA is contained in the PIDA Overview which can be found in the Human Resources section on ICON.

## 11. Glossary

- 11.1 'Malpractice' – in the context of this policy this may refer to any of the following:

- Failure to comply with a legal obligation
- Unprofessional acts
- Misuse or inappropriate use of ICO funds or resources
- A criminal offence
- A miscarriage of justice
- The endangering of an individual's health and safety
- Damage to the environment

- Deliberate concealment of information relating to any of the above

# **Security Manual**

## **Security Incidents**

### **Introduction**

The ICO treats all security incidents seriously. It is important that staff report all security incidents even if they seem trivial. This advice is intended to give guidance to staff on the most appropriate person to report an incident depending on its nature.

### **Scope**

The ICO is responsible for, and handles, a wide range of assets that require protection. 'Assets' include:

- People and their knowledge, skills and experience.
- Anything valuable for which the office is responsible, including all buildings, property and material, such as cash, furniture, equipment.
- Information, including records in all forms, whether held electronically or digitally, on paper, disk, microfiche, audio tape.

In order to protect these assets we should ensure that a good level of security surrounds them. Where there is evidence of a breach of that security it is important that this is reported immediately in the most appropriate manner. This will ensure that we can deal with it quickly and take appropriate steps to prevent any recurrence.

There are a number of different types of incident which could constitute a potential breach of security. Some of them will be obvious such as the loss of data or an access swipe card or a virus on your computer, however, some may be less obvious. Examples of possible IT and general security incidents are set out below, but these are only given as a guide.

### **Examples of IT security incidents**

- theft of hardware, software or information.
- loss of hardware, software or information.
- deliberate damage to equipment.
- abusing IT privileges, such as using someone else's password.

- unauthorised access to information held on a computer, including overlooking.
- Making unauthorised amendments to software installed on a computer.
- Disclosing information to an unauthorised person.
- A computer virus or viruses infecting the network
- Copying software without permission
- Using a networked computer for personal matters or playing games.
- User or admin error causing disruption to the service.
- A key hardware failure causing disruption to service.

## Examples of general security incidents

- An unauthorised person accessing or attempting to gain access to the building or secure areas.
- Disclosing or losing personal data or information provided for work purposes.
- Bomb threats - whether face to face, on the telephone or in writing.
- Suspect packages found inside or outside any of ICO's buildings.
- An assault on a member of staff or on the ICO's premises.
- Vandalism that could allow security to be breached.
- An intruder detection alarm being activated
- Unauthorised activation of the fire alarm.
- Losing a security pass or access swipe card
- Theft.

## How to report a suspected security incident

If you suspect that there has been or may be a breach of security you should report it immediately, even if it is only a suspicion. Follow the reporting procedure described below. You should also inform your line manager. If your line manager is not available, you should inform another manager as soon as possible. The follow on action will depend on the type of incident and the impact that this could cause.

## Breach of IT security

Report immediately to the Northgate service desk on 6111 or 08000 778 490 and then your manager.

## Bomb threats and suspicious packages

**Always report a suspicious object or package or bomb threat (verbal or written) to a member of [Information Security](#) or [Facilities Management](#)**

Instructions will be given to staff over the public address system if this proves necessary.

## Assaults or theft

This should be reported to your **immediate line manager** and then to a member of the [Information Security Team](#).

## Loss of security pass

Complete the lost pass [form](#) on ICON and send to [Information Security](#) and [Facilities Management](#).

If you find a security pass you should hand this in to the [Facilities Manager](#).

New cards can be obtained from the [Facilities Management Department](#).

## Activation of fire alarm or intruder alarm

Familiarise yourself with the fire alarm procedures in particular and follow them if the alarm is raised.

If you suspect someone has set off the fire alarm to gain unauthorised access to the building you should inform a member of the [Information Security Team](#).

## Any other type of incident

When you become aware of any situation you elieve would potentially cause a breach of security, you should report this immediately to a member of the [Information Security Team](#). Do not wait for your own line manager to become available.

In order to report any incident, contact a member of the [Information Security Team](#), either by phone or email: [infosec@ico.org.uk](mailto:infosec@ico.org.uk).